

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-092040

(43)Date of publication of application : 31.03.2000

(51)Int.Cl.

H04L 9/10

B42D 15/10

G06K 17/00

G07B 15/00

H04L 9/14

H04L 9/32

(21)Application number : 10-258016

(71)Applicant : OMRON CORP

(22)Date of filing : 11.09.1998

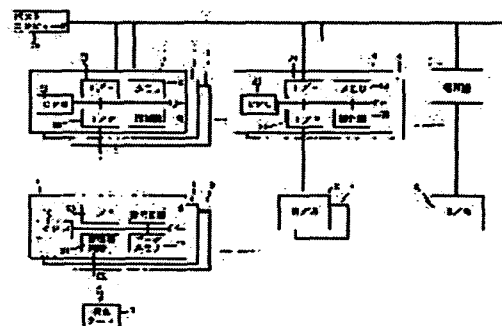
(72)Inventor : WAKABAYASHI NAOYUKI

**(54) STORAGE MEDIUM, READER/WRITER, CARD SYSTEM, METHOD FOR USING CRYPTOGRAPHIC KEY, STATION SERVICE SYSTEM, AND CARD ISSUING MACHINE**

(57)Abstract:

**PROBLEM TO BE SOLVED:** To update a cryptographic key as required, e.g. periodically or in case of possibility of a decoded cryptographic key without using all cryptographic keys at random by updating the cryptographic key selected by a command sent from a reader/writer.

**SOLUTION:** A reader/writer 6 stores old cryptographic keys that were used in the past and not in use at present and a cryptographic key that is currently in use. Furthermore, the reader/writer 6 transmits an update command to a passenger card 7 to allow the passenger card 7 to update its cryptographic key from an older cryptographic key to the cryptographic key used at present when the cryptographic key used by the passenger card 7 is the cryptographic key that was used in the past but not in use at present according to a response from the passenger card 7 as a result of communication between the reader/writer 6 and the passenger card 7, and the passenger card 7 updates the cryptographic key into the cryptographic key used at present in response to the command. Thus, the cryptographic key of the old passenger card 7 having been issued before is finally updated into the cryptographic key used at present.



## LEGAL STATUS

[Date of request for examination] 03.09.1999

[Date of sending the examiner's decision of rejection] 08.08.2000

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-92040

(P2000-92040A)

(43) 公開日 平成12年 3月31日 (2000.3.31)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
H 0 4 L 9/10		H 0 4 L 9/00	6 2 1 A 2 C 0 0 5
B 4 2 D 15/10	5 2 1	B 4 2 D 15/10	5 2 1 5 B 0 5 8
G 0 6 K 17/00		G 0 6 K 17/00	S 5 J 1 0 4
G 0 7 B 15/00	5 1 0	G 0 7 B 15/00	5 1 0
H 0 4 L 9/14		H 0 4 L 9/00	6 4 1

審査請求 有 請求項の数10 O L (全 13 頁) 最終頁に続く

(21) 出願番号 特願平10-258016

(22) 出願日 平成10年 9月11日 (1998.9.11)

(71) 出願人 000002945

オムロン株式会社

京都府京都市右京区花園土堂町10番地

(72) 発明者 若林 尚之

京都府京都市右京区花園土堂町10番地 オムロン株式会社内

(74) 代理人 100086737

弁理士 岡田 和秀

Fターム(参考) 2C005 MA03 MB07 NA09 SA02 SA03

SA05 SA06 SA07 TA21 TA22

5B058 KA11 KA33 KA35 YA20

5J104 AA16 EA02 EA18 NA02 NA33

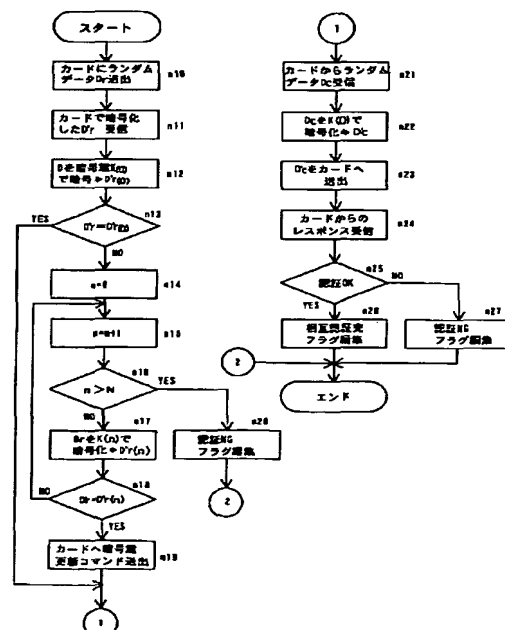
PA11

(54) 【発明の名称】 記憶媒体、読出／書込機、カードシステム、暗号鍵使用方法、駅務システムおよびカード発行機

(57) 【要約】

【課題】 ICカードなどの記憶媒体と読出／書込機との間の暗号処理などにおいて、使用する暗号鍵を、必要な時に更新できるとともに、複数の暗号鍵の全てが解読される危険性が低く、記憶媒体に記憶させている複数の暗号鍵を変更することができるようにする。

【解決手段】 ICカードには、ICカード発行時に、そのICカード発行時点で使用している暗号鍵および今後使用する予定の暗号鍵の複数の暗号鍵を記憶させ、読出／書込機には、現在使用している暗号鍵と過去に使用した旧い複数の暗号鍵とを記憶させ、読出／書込機は、ICカードからのレスポンスによって、ICカードが使用している暗号鍵が、過去に使用した暗号鍵であるときには、現在使用している暗号鍵に更新するように更新コマンドを送出し、ICカードは、そのコマンドに応答して使用する暗号鍵を更新するように構成している。



【特許請求の範囲】

【請求項 1】 暗号鍵を用いて読出／書込機との間で認証および通信を行うよう構成された記憶媒体において、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記読出／書込機から送出されるコマンドにより前記選択する暗号鍵を更新する暗号鍵更新手段とを具備したことを特徴とする記憶媒体。

【請求項 2】 請求項 1 において、前記暗号鍵記憶手段に記憶されている複数の暗号鍵の少なくとも一部の暗号鍵を読出／書込機から書き換えることを特徴とする記憶媒体。

【請求項 3】 暗号鍵を用いて記憶媒体との間で認証および通信を行うよう構成された読出／書込機において、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記記憶媒体からのレスポンスにより該記憶媒体が現在使用している暗号鍵が、当該読出／書込機で過去に使用された暗号鍵であるかどうかを知る暗号鍵知得手段と、前記記憶媒体が現在使用している暗号鍵が過去に使用された暗号鍵のときは、前記記憶媒体の暗号鍵を更新するコマンドを送出する暗号鍵更新コマンド送出手段とを具備したことを特徴とする読出／書込機。

【請求項 4】 請求項 3 において、上位機器からのコマンドにより、当該読出／書込機が使用する暗号鍵を変更する暗号鍵変更手段を具備したことを特徴とする読出／書込機。

【請求項 5】 請求項 3 において、前記記憶媒体が記憶している複数の暗号鍵の少なくとも一部の暗号鍵を書き換えることを特徴とする読出／書込機。

【請求項 6】 請求項 1 または 2 に記載の記憶媒体をカードとし、該カードと、請求項 3 ないし 5 いずれかに記載の読出／書込機とを有し、カードが現在使用している暗号鍵が、前記読出／書込機で過去に使用された暗号鍵のときは、カードの暗号鍵を更新した後、その更新された暗号鍵を用いてカードと読出／書込機とが相互認証を行うことを特徴とするカードシステム。

【請求項 7】 記憶媒体と読出／書込機それぞれには複数の暗号鍵を記憶させておき、読出／書込機は、記憶媒体から送信されてきた該記憶媒体が使用している暗号鍵による暗号化データと、読出／書込機が使用している暗号鍵により作成した暗号化データとを比較して記憶媒体および読出／書込機が使用している暗号鍵が一致しているか否かを判断し、一致していないときには、記憶媒体から送信されてきた前記暗号化データと、読出／書込機で過去に使用した暗号鍵により作成した暗号化デ

ータとを比較して記憶媒体が現在使用している暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、前記過去に使用した暗号鍵であるときには、記憶媒体に対して、該記憶媒体が使用している暗号鍵を更新させる更新コマンドを送信し、

記憶媒体は、前記更新コマンドに応答して、暗号鍵を更新することを特徴とする暗号鍵使用方法。

【請求項 8】 請求項 1 または 2 に記載の記憶媒体を乗車カードとし、該乗車カードと、これに対する読み出し／書き込みを行う請求項 3 または 4 に記載の読出／書込機を備えた自動改札機とを有し、

読出／書込機は、

乗車カードから送信されてきた該乗車カードが使用している暗号鍵による暗号化データと、読出／書込機が使用している暗号鍵により作成した暗号化データとを比較して乗車カードおよび読出／書込機が使用している暗号鍵が一致しているか否かを判断し、一致していないときには、乗車カードから送信されてきた前記暗号化データ

と、読出／書込機で過去に使用した暗号鍵により作成した暗号化データとを比較して乗車カードが使用している暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、過去に使用した暗号鍵であるときには、乗車カードに対して、該乗車カードが使用している暗号鍵を更新させる更新コマンドを送信し、

乗車カードは、前記更新コマンドに応答して、暗号鍵を更新することを特徴とする駅務システム。

【請求項 9】 請求項 1 または 2 に記載の記憶媒体を乗車カードとし、該乗車カードと、これに対する読み出し／書き込みを行う請求項 5 に記載の読出／書込機を備えたカード発行機とを有し、

読出／書込機は、乗車カードの発行時に、該乗車カードに記憶されている複数の暗号鍵を書き換えることを特徴とする駅務システム。

【請求項 10】 請求項 1 または 2 に記載の記憶媒体を乗車カードとし、該乗車カードの暗号鍵記憶手段に、現在使用する暗号鍵および将来使用する予定の複数の暗号鍵を書き込む一方、暗号鍵選択手段で前記現在使用する暗号鍵を選択するように設定して該乗車カードを発行するカード発行機。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、データを記憶する記憶媒体、この記憶媒体に対して読み出し／書き込みを行う読出／書込機、それらを用いたカードシステム、それらに好適な暗号鍵使用方法、および、それらを用いた自動改札などの駅務システム並びにカード発行機に関する。

【0002】

【従来の技術】例えば、記憶媒体であるカードを自動料金徴収機の読出／書込機でカードの入出金などの処理をする場合、カードのセキュリティ性を確保する必要がある。そのため、通常、カードと読出／書込機との間で暗号を用いた相互認証や通信の暗号化が行われている。なお、相互認証とは、カード側からみて、通信相手となる読出／書込機が正当であるか、また読出／書込機側からみて、通信相手であるカードが正当であるかを、相互に認証することであるが、通常、相互に相手が正当な暗号鍵を知っているかどうかで判定する。

【0003】

【発明が解決しようとする課題】上述の暗号処理においては、すべてのカードおよび読出／書込機も同じ暗号鍵（共通暗号鍵）を使用するようにした方式があるが、この方式では一旦、共通暗号鍵が他人に知られると、システム全体のセキュリティ性が損なわれてしまうという欠点がある。

【0004】この欠点をなくすために、カードに複数の暗号鍵を記憶させ、また読出／書込機にもカードが有する複数の暗号鍵を記憶させておき、読出／書込機側ではカードとの間の暗号処理において、前記複数の暗号鍵のうちのいずれか1つの暗号鍵をランダムに用いることでセキュリティ性を高められるようにしたシステムがある。

【0005】こうした場合に問題とされているのは、前記ランダムに暗号鍵を用いているうちに、複数の暗号鍵のすべてが傍受され解読されてしまう危険性があり、特に、カードと読出／書込機とが非接触で通信を行う場合に、その危険性が増大する。そこで、カードが記憶する複数の暗号鍵のすべてを他の複数の暗号鍵に一斉に変更させることが考えられるが、このような暗号鍵の変更は、多数のカードが発行されて使用されるというカードの利用形態から考えて実際上は不可能である。

【0006】本発明は、上述の技術的課題に鑑みて為されたものであって、ランダムにすべての暗号鍵を使用するのではなく、必要な時、例えば、定期的あるいは暗号鍵が解読されたような虞れがある時に暗号鍵を更新できるようにし、しかも、記憶媒体の複数の暗号鍵の変更を一斉に行う必要がないようにすることを目的とする。

【0007】

【課題を解決するための手段】本発明では、上述の目的を達成するために、次のように構成している。

【0008】すなわち、請求項1の本発明の記憶媒体は、暗号鍵を用いて読出／書込機との間で認証および通信を行うよう構成された記憶媒体において、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記読出／書込機から送出されるコマンドにより前記選択する暗号鍵を更新する暗号鍵更新手段とを具備している。

【0009】ここで、更新とは、使用している暗号鍵を、複数の暗号鍵の内の別の暗号鍵に切り換えて使用することをいい、更新の度に、複数の暗号鍵の内の一つの暗号鍵が、それまで使用していた暗号鍵に代えて使用されることになる。

【0010】また、記憶媒体と読出／書込機との間の通信は、有線方式または無線方式のいずれの方式であってもよい。

【0011】請求項2の本発明の記憶媒体は、請求項1において、前記暗号鍵記憶手段に記憶されている複数の暗号鍵の少なくとも一部の暗号鍵を読出／書込機から書き換えるものである。

【0012】請求項3の本発明の読出／書込機は、暗号鍵を用いて記憶媒体との間で認証および通信を行うよう構成された読出／書込機において、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記記憶媒体からのレスポンスにより該記憶媒体が現在使用している暗号鍵が、当該読出／書込機で過去に使用された暗号鍵であるかどうかを知る暗号鍵知得手段と、前記記憶媒体が現在使用している暗号鍵が過去に使用された暗号鍵のときは、前記記憶媒体の暗号鍵を更新するコマンドを送出する暗号鍵更新コマンド送出手段とを具備している。

【0013】請求項4の本発明の読出／書込機は、請求項3において、上位機器からのコマンドにより、当該読出／書込機が使用する暗号鍵を変更する暗号鍵変更手段を具備している。

【0014】請求項5の本発明の読出／書込機は、請求項3において、前記記憶媒体が記憶している複数の暗号鍵の少なくとも一部の暗号鍵を書き換えるものである。

【0015】請求項6の本発明のカードシステムは、請求項1または2に記載の記憶媒体をカードとし、該カードと、請求項3ないし5いずれかに記載の読出／書込機とを有し、カードが現在使用している暗号鍵が、読出／書込機で過去に使用された暗号鍵のときは、カードの暗号鍵を更新した後、その更新された暗号鍵を用いてカードと読出／書込機とが相互認証を行うものである。

【0016】請求項7の本発明の暗号鍵使用法は、記憶媒体と読出／書込機それぞれには複数の暗号鍵を記憶させておき、読出／書込機は、記憶媒体から送信されてきた該記憶媒体が使用している暗号鍵による暗号化データと、読出／書込機が使用している暗号鍵により作成した暗号化データとを比較して記憶媒体および読出／書込機が使用している暗号鍵が一致しているかを判断し、一致していないときには、記憶媒体から送信されてきた前記暗号化データと、読出／書込機で過去に使用した暗号鍵により作成した暗号化データとを比較して記憶媒体が使用している暗号鍵が、過去に使用した暗号鍵であるかを判断し、過去に使用した暗号鍵であるとき

には、記憶媒体に対して、該記憶媒体が使用している暗号鍵を更新させる更新コマンドを送信し、記憶媒体は、前記更新コマンドに应答して、暗号鍵を更新するものである。

【0017】請求項8の本発明の駅務システムは、請求項1または2に記載の記憶媒体を乗車カードとし、該乗車カードと、これに対する読み出し／書き込みを行う請求項3または4に記載の読出／書込機を備えた自動改札機とを有し、読出／書込機は、乗車カードから送信されてきた該乗車カードが使用している暗号鍵による暗号化データと、読出／書込機が使用している暗号鍵により作成した暗号化データとを比較して乗車カードおよび読出／書込機が使用している暗号鍵が一致しているか否かを判断し、一致していないときには、乗車カードから送信されてきた前記暗号化データと、読出／書込機で過去に使用した暗号鍵により作成した暗号化データとを比較して乗車カードが使用している暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、過去に使用した暗号鍵であるときには、乗車カードに対して、該乗車カードが使用している暗号鍵を更新させる更新コマンドを送信し、乗車カードは、前記更新コマンドに应答して、暗号鍵を更新するものである。

【0018】請求項9の本発明の駅務システムは、請求項1または2に記載の記憶媒体を乗車カードとし、該乗車カードと、これに対する読み出し／書き込みを行う請求項5に記載の読出／書込機を備えたカード発行機とを有し、読出／書込機は、乗車カードの発行時に、該乗車カードに記憶されている複数の暗号鍵を書き換えるものである。

【0019】請求項10の本発明のカード発行機は、請求項1または2に記載の記憶媒体を乗車カードとし、該乗車カードの暗号鍵記憶手段に、現在使用する暗号鍵および将来使用する予定の複数の暗号鍵を書き込む一方、暗号鍵選択手段で前記現在使用する暗号鍵を選択するように設定して該乗車カードを発行するものである。

【0020】（作用）請求項1の記憶媒体によれば、読出／書込機との間の暗号処理において、複数の暗号鍵のいずれかをを用いて暗号処理を行うので、共通暗号鍵方式のように一つの共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、全ての暗号鍵が傍受されて解読される虞れが低い。

【0021】請求項2の記憶媒体によれば、記憶されている複数の暗号鍵が更新によって全て使用されてしまうまでに、複数の暗号鍵の少なくとも一部の暗号鍵を読出／書込機から新たな暗号鍵に書き換えることができる。これによって、永続的に新しい暗号鍵への更新が可能となる。

【0022】請求項3の読出／書込機によれば、記憶媒体が使用している暗号鍵が、読出／書込機で過去に使用された暗号鍵であるか否かを判断し、過去に使用されている暗号鍵であるときには、記憶媒体に更新コマンドを送出して記憶媒体が使用する暗号鍵を更新することができるので、記憶媒体の暗号鍵を、読出／書込機が現在使用している最新の暗号鍵に一致させることができる。

【0023】請求項4の読出／書込機によれば、上位機器からのコマンドによって使用する暗号鍵が変更されるので、必要に応じて、例えば、定期的あるいは現在使用している暗号鍵が解読される虞れがあるような時に、上位機器からのコマンドによって使用する暗号鍵を、新しい暗号鍵に変更できることになり、さらに、請求項3の作用によって、記憶媒体が使用する暗号鍵もその変更された暗号鍵に一致させることができる。

【0024】請求項5の読出／書込機によれば、記憶媒体が記憶している複数の暗号鍵の少なくとも一部の暗号鍵を書き換えるので、記憶媒体の暗号鍵が順次更新されて記憶されている全ての暗号鍵が使用されてしまうまでに、新たな暗号鍵に書き換えることができ、これによって、永続的に新しい暗号鍵への更新が可能となる。

【0025】請求項6のカードシステムによれば、カードと読出／書込機との暗号鍵が一致しなくても、カードの暗号鍵が、過去に使用した暗号鍵であれば、カードの暗号鍵が更新されて読出／書込機の暗号鍵に一致するので、相互認証が可能となる。

【0026】請求項7の暗号鍵使用方法によれば、読出／書込機は、記憶媒体からの暗号化データと作成した暗号化データとを比較することにより、記憶媒体の暗号鍵が、読出／書込機が使用している暗号鍵に一致しているか否かを判断し、一致していないときには、記憶媒体の暗号鍵が、読出／書込機で過去に使用した暗号鍵であるか否かを判断し、過去の暗号鍵であるときには、記憶媒体の暗号鍵を更新させるので、記憶媒体の暗号鍵と読出／書込機との暗号鍵を一致させることができる。

【0027】請求項8の駅務システムによれば、乗車カードと自動改札機の読出／書込機との間の暗号処理において、乗車カードおよび読出／書込機は、複数の暗号鍵を記憶しているので、一つの共通暗号鍵のみを記憶している共通暗号鍵方式のように共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、すべての暗号鍵が傍受されて解読される虞れが低い。

【0028】請求項9の駅務システムによれば、カード発行機は、乗車カードの発行時に、乗車カードに記憶されている複数の暗号鍵を書き換えるので、永続的に新しい暗号鍵への更新が可能となる。

【0029】請求項10のカード発行機によれば、それ

まで使用された乗車カードを回収して新たな乗車カードとして発行するのではなく、使用されたことのない全く新規な乗車カードの発行時において、相互認証などを行うことなく、現在使用する暗号鍵および将来使用する予定の複数の暗号鍵を書き込むとともに、現在使用する暗号鍵を選択するよう設定して乗車カードを発行できる。

【0030】

【発明の実施の形態】以下、図面によって本発明の実施の形態について詳細に説明する。

【0031】図1は、本発明が適用される駅務システムの全体構成を示す図であり、同図において、7は記憶媒体（例えば、非接触通信ICカード）としての定期券などの乗車カード、6はこの乗車カード7との間で非接触通信を行う読出／書込機（リーダ／ライタ）、1は読出／書込機6を備えた自動改札機、4は読出／書込機6を備えたカード発行機、5は読出／書込機6を備えた精算機であり、25はこれらを制御するホストコンピュータである。自動改札機1および精算機4は、駅の構内に、複数台設置されている。

【0032】乗車カード7は、カード発行機4で発行される。この発行された乗車カード7には、乗車区間とか使用有効期限等のデータが記録される。利用者は、発行された乗車カードやを用いて自動改札機1の改札を受ける。カード発行機4も自動改札機1も読出／書込機6を備えている。カード発行機4および自動改札機1は、読出／書込機6に対する上位機器となる。また、ホストコンピュータ25は、カード発行機4および自動改札機1などに対する上位機器となる。自動改札機1は、CPU26、ホストコンピュータ25および読出／書込機6との間のインタフェース回路27、28、メモリ29および制御回路30などを備えており、カード発行機4は、CPU31、ホストコンピュータ25および読出／書込機6との間のインタフェース回路32、33、メモリ34およびカード発行のための操作盤35などを備えている。なお、読出／書込機6を構成するブロックには、後述の説明で使用する参照符号を付している。

【0033】ここで、システムの主要な構成の説明に先立って、この実施の形態の暗号鍵の使用方法についての概要を説明する。

【0034】乗車カード7と読出／書込機6との間では、セキュリティ性を確保するために、暗号鍵を用いた認証や通信を行うのであるが、この実施の形態では、従来例の暗号処理方式の欠点を解消するために、次のように構成している。

【0035】すなわち、乗車カード7には、カード発行時に、今後使用する予定の複数の暗号鍵を記憶させておき、その複数の暗号鍵の内の予め定めた暗号鍵（例えば、カード発行時点において使用すべき暗号鍵）を使用するように設定しておき、読出／書込機6からの更新コマンドがあったときには、そのコマンドで指定された暗

号鍵に更新してその更新された暗号鍵を使用するように構成している。

【0036】乗車カード7は、多数が長い期間に亘って順次的に発行されるために、乗車カード7に記憶される複数の暗号鍵の内容も必要に応じて新しい暗号鍵に順次的に切り換えられ、したがって、当初に発行された乗車カード7に記憶されている複数の暗号鍵（例えば、K1、K2、K3、K4、K5）と、後に発行される乗車カード7に記憶される複数の暗号鍵（例えば、K2、K3、K4、K5、K6）とは、共通する暗号鍵（K2、K3、K4、K5）が存在するけれども、当初の乗車カード7には、後の乗車カード7に記憶されていない古い暗号鍵（K1）が記憶されている一方、後の乗車カード7には、当初の乗車カード7に記憶されていない将来使用する予定の新規な暗号鍵（K6）が記憶される場合が生じることになる。

【0037】そして、全ての乗車カード7に共通に記憶されている複数の暗号鍵が、使用可能な暗号鍵となり、その複数の暗号鍵が順番で使用されることになる。

【0038】一方、読出／書込機6には、過去に使用されて現在は使用されていない古い暗号鍵（例えば、K1）および現在使用されている暗号鍵（例えば、K2）が少なくとも記憶されており、この暗号鍵（例えばK2）を使用する。

【0039】さらに、読出／書込機6では、乗車カード7との間の通信において、乗車カード7のレスポンスからその乗車カード7が使用している暗号鍵が、過去に使用されて現在使用されていない暗号鍵（例えばK1）であれば、乗車カード7に対して、現在使用されている暗号鍵（例えばK2）に更新するように更新コマンドを送出し、これに応答してその乗車カード7は、現在使用されている暗号鍵（例えばK2）に更新するのである。

【0040】したがって、当初発行された古い乗車カード7は、読出／書込機6との通信によって、最終的に現在使用されている暗号鍵（例えばK2）に更新されて統一されることになる。

【0041】システムのセキュリティ性を確保するために、定期的に、あるいは、現在使用されている暗号鍵が解読された虞れがあるような時には、上位機器である自動改札機1などからの変更コマンドによって、読出／書込機6は、現在使用している暗号鍵（例えば、K2）を、次に使用すべき暗号鍵（例えば、K3）に変更する一方、それまで使用していた暗号鍵（K2）を、古い暗号鍵として追加し、以後、この変更した暗号鍵（K3）を使用する。したがって、この時点では、読出／書込機6には、過去に使用して現在使用されていない複数の暗号鍵（例えば、K1、K2）および現在使用されている暗号鍵（例えば、K3）が記憶されることになる。

【0042】上位機器からの変更コマンドによって暗号鍵を変更した読出／書込機6と乗車カード7との通信に

よって、乗車カード7が、現在使用されていない過去に使用されていた暗号鍵（例えば、K2）を使用していたときには、読出／書込機6は、その乗車カード7に対して、現在使用されている暗号鍵（例えばK3）に更新するように更新コマンドを送出し、これに応答してその乗車カード7は、現在使用されている暗号鍵（例えばK3）に更新するのである。

【0043】したがって、乗車カード7は、読出／書込機6との通信によって、最終的に現在使用されている暗号鍵（例えばK3）に更新されて統一されることになる。

【0044】このように複数の暗号鍵を必要に応じて順次更新して暗号処理を行うので、共通暗号鍵方式のように一つの共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機6からの更新コマンドによって必要に応じて更新されるので、ランダムに全ての暗号鍵を用いる従来例のように、全ての暗号鍵が傍受されて解読される虞れが低い。

【0045】さらに、乗車カード7の暗号鍵の更新も、読出／書込機6との通信による更新コマンドによって行われるので、全ての乗車カード7の複数の暗号鍵を一斉に変更するといった必要がない。

【0046】以下、この乗車カード7および読出／書込機6等の主要な構成について詳細に説明する。

【0047】図2は、この実施の形態の読出／書込機を備えた自動改札機1の外観斜視図であり、この自動改札機1は、改札通路36を隔てて相対向する一対の改札機本体2を備える。両改札機本体2の側面それぞれには、改札通路36の通過を許可あるいは阻止する図示しない扉が配備されている。各改札機本体2には、読出／書込機6が設けられており、そのアンテナコイル23が各改札機本体2の上面に臨むように配設されている。

【0048】このアンテナコイル23は、定期券等の乗車カード7が備えるアンテナコイルが通信エリア内に位置したときに、その乗車カード7のアンテナコイルとの間で非接触でデータ通信が可能となっている。乗車カード7を携帯する利用者は、図2に示すように、その乗車カード7を改札機本体2に設けられた読出／書込機6のアンテナコイル23との通信のための通信エリアにかざすだけでデータ通信が可能となる。

【0049】読出／書込機6は乗車カード7と通信を行い、上位機器である自動改札機1は、その通信に基づいて乗車カード7の真偽および乗車条件などを判定し、これに基づいて、扉を制御して開放したり、閉止したりする。

【0050】本実施の形態の乗車カード7は、上述のように複数の暗号鍵を記憶しており、それら複数の暗号鍵の中からある1つの暗号鍵を用いて暗号化とか復号化を行い、また、自動改札機1の読出／書込機6の更新コマ

ンドにより現在使用している暗号鍵を次に使用する暗号鍵に更新し、またカード発行機4などの読出／書込機によって、カード発行時に、記憶している複数の全ての暗号鍵が書き換えられるようにしている。なお、カード発行時には、乗車カード7の複数の暗号鍵の全てではなく、使用済みの暗号鍵のみを新たな暗号鍵に書き換えるようにしてもよい。

【0051】以下、図3を参照して、乗車カード7について説明する。乗車カード7は、内部にCPU8、プログラムメモリ9、データメモリ10、暗号鍵記憶メモリ11、暗号回路12および変復調電源回路13ならびにアンテナコイル14を有している。

【0052】CPU8は、プログラムメモリ9に格納されているプログラムデータと、データメモリ10に格納されているワーキングデータとを用いて、アンテナコイル14を通じて受信した読出／書込機6からのコマンドに基づく処理を行うとともに、読出／書込機6に対してデータ送信の処理を行う。

【0053】カード読出／書込機6から乗車カード7に送出されてくるコマンドには、ポーリング、認証、データの読み出しと書き込み、禁止などがある。CPU8は、カード読出／書込機6からのこうした送出コマンドをアンテナコイル14で受信し、変復調回路13で復調し、暗号回路12で復号する等の処理を行わせた後に取り込んで解析するとともに、この解析したコマンドに従った処理を実行するようになっている。

【0054】暗号鍵記憶メモリ11には、暗号鍵記憶手段として、図4で示すように乗車カード7の発行時に、カード発行機4の読出／書込機6によって、乗車カード7が自動改札機1の読出／書込機6などとの間で今後使用する予定である複数の暗号鍵（暗号鍵1、暗号鍵2、暗号鍵3、…、暗号鍵n）が記憶させられている。暗号鍵記憶メモリ11からは、これら複数の暗号鍵の読み出しは外部から一切できないハードウェア構成とされて不正に外部から暗号鍵が読み出せないようになっている。このハードウェア構成は、暗号鍵記憶メモリ11をCPU8と同じLSIチップに設け、このLSIチップにテストピンを当てて信号を与えても暗号鍵は出力されず、あるいは、テスト端子をなくし、暗号鍵記憶メモリ11からのデータの読み出しは、LSIチップ内のCPU8のみができるようにし、CPU8と暗号鍵記憶メモリ11間のバスは、LSIチップの外には、端子として出さないようにすればよい。これによって、LSIチップの外部（回路の外）から暗号鍵の読み出しを一切できないようにすることができる。

【0055】CPU8は、暗号鍵選択手段として、暗号鍵記憶メモリ11に記憶されている図4の暗号鍵1、暗号鍵2、暗号鍵3、…、暗号鍵nから予め設定されている1つの暗号鍵を選択し、これを暗号回路12に入力するようになっている。通常、カード発行時には、その時

点で使用されている暗号鍵 1 と、今後順番に使用されていく予定の複数の暗号鍵 2, 3, ... が記憶させられるので、当初は、暗号鍵 1 を使用すべき暗号鍵として設定されている。

【0056】その後、自動改札機 1 の読出／書込機 6 から更新コマンドがあれば、CPU 8 は、暗号鍵更新手段として、そのコマンドに従って現在設定されている暗号鍵から更新コマンドで指定された他の暗号鍵に設定を更新したうえで、これを暗号回路 12 に入力するようになっている。

【0057】暗号回路 12 は、上述のようにして選択された暗号鍵を用いて暗号化、復号化を行うものであり、自動改札機 1 の読出／書込機 6 との相互認証においても使用される。勿論、本実施の形態における乗車カード 7 は読出／書込機 6 との間での相互認証の後でのみデータの読み出しや書き込みのコマンドを受け付けるようになっている。

【0058】変復調電源回路 13 は、自動改札機 1 の読出／書込機 6 へ送信するデータの変調、読出／書込機 6 から受信したデータの復調、アンテナコイル 14 で受けた読出／書込機 6 からの送信磁界により乗車カード 7 の電源を生成するようになっている。

【0059】本実施の形態の読出／書込機 6 は、暗号鍵を用いて乗車カード 7 との間で認証および通信を行うよう構成されたものであって、複数の暗号鍵を記憶する暗号鍵記憶手段と、前記暗号鍵記憶手段に記憶されている複数の暗号鍵のうちからいずれかを選択する暗号鍵選択手段と、前記乗車カードからのレスポンスにより乗車カードで現在使用されている暗号鍵が、過去に使用されたいずれの暗号鍵であるかを知る暗号鍵知得手段と、乗車カードで現在使用されている暗号鍵が過去に使用されていた暗号鍵のときは、乗車カードの暗号鍵を更新するコマンドを送出するコマンド送出手段と、上位機器からのコマンドにより、当該読出／書込機が使用する暗号鍵を変更する暗号鍵変更手段とを具備している。

【0060】以下、図 5 を参照して読出／書込機 6 について説明する。この読出／書込機 6 は、CPU 15、プログラムメモリ 16、データメモリ 17、暗号回路 18、乗車カード用暗号鍵記憶メモリ 19、上位機器用暗号鍵記憶メモリ 20、上位機器用インタフェース 21 および変復調回路 22 ならびにアンテナコイル 23 を有している。上位機器とは、上述のように、自動改札機 1 あるいはカード発行機 4 などである。

【0061】自動改札機 1 は、読出／書込機 6 の他に扉の駆動機構を制御したり、ホストコンピュータ 25 と通信を行うものであり、読出／書込機 6 の上位機器用インタフェース 21 を介して接続されている。

【0062】読出／書込機 6 は、電源投入時に、上位機器である自動改札機 1 などとの間でも相互認証を行い、接続のセキュリティ性を確保し、それ以降の自動改札機

などの上位機器におけるアプリケーションに応じた処理を行うようになっている。

【0063】システムのセキュリティ性を確保するために、現在使用されている暗号鍵の使用期間が一定期間に達したり、あるいは、現在使用されている暗号鍵が解読された虞れがあるような場合には、例えば、ホストコンピュータ 25 から上位機器である自動改札機 1 などを通して読出／書込機 6 の CPU 15 に対して、現在使用している暗号鍵を変更するコマンドが与えられ、これによって、乗車カード用暗号鍵記憶メモリ 19 の暗号鍵が後述のように書き換えられて変更される。その後、読出／書込機 6 は、変更した暗号鍵で乗車カード 7 との処理を行うようになっている。

【0064】図 6 は、暗号鍵の使用期間の一例を示す図であり、この例は、暗号鍵の解読といった事態が生じることなく順調に経過すれば、三カ月毎に暗号鍵を変更するものであり、暗号鍵 1 は、1998 年 1 月 1 日から同年 3 月 31 日までの三カ月間既に使用され、その後、暗号鍵 2 が現在使用中であり、順調に経過すれば、1998 年 6 月 30 日まで暗号鍵 2 が使用される予定であり、1998 年 7 月 1 日からは暗号鍵 3 に変更されて暗号鍵 3 が使用される予定である。

【0065】次に、読出／書込機 6 の動作について説明する。読出／書込機 6 は、上位機器用インタフェース 21 を通して自動改札機 1 などの上位機器から受信したコマンドを復号し、復号したコマンドを CPU 15 で解析し、そのコマンドに従った処理を実行する。上位機器からのコマンドが、例えば乗車カード 7 のデータメモリ 10 に記憶されている乗車カード 7 に関するデータ、例えば定期券の有効期間、定期券の乗車区間というデータを読み出すというコマンドであれば、乗車カード 7 のデータメモリ 10 からデータを読み取るリードコマンドを、乗車カード用暗号鍵記憶メモリ 19 から選択した暗号鍵を用いて暗号回路 18 で暗号化させ、変復調回路 22 で変調させたうえでアンテナコイル 23 から乗車カード 7 に送信する。そして、乗車カード 7 から前記リードコマンドに対して返送されるレスポンスを受信すると、それを変復調回路 22 で復調し、暗号回路 18 で復号したうえで乗車カード 7 のデータを得る。そして、そのデータを、暗号回路 18 で暗号化してレスポンスとして上位機器用インタフェース 21 から上位機器に送信する。そして、上位機器、例えば自動改札機 1 は、このレスポンスから乗車カード 7 が正当であれば開閉ドアを開け、正当でなければ開閉ドアを開けないように制御する。

【0066】ここで、読出／書込機 6 から乗車カード 7 に与えられるコマンドにはポーリング、認証、データの読み出しと書き込みなどの従来からのコマンドの他に、乗車カード 7 の暗号鍵更新コマンド、乗車カード 7 の暗号鍵書き換えコマンドがある。また、上位機器である自動改札装置やカード発行機などからのコマンドには、乗

車カード7との通信コマンド、認証、カード読出／書込機6に対するデータの読み出しと書き込みなどの従来からのコマンドの他に、乗車カード7の暗号鍵更新コマンド、乗車カード7の暗号鍵書き換えコマンド、カード読出／書込機6の暗号鍵書き換えコマンドがある。

【0067】乗車カード用暗号鍵記憶メモリ19は、図7で示すように乗車カード7との間で過去に使用していた暗号鍵（旧暗号鍵-m, ..., 旧暗号鍵-1）と現在使用している暗号鍵（現在の暗号鍵0）とが記憶されている。乗車カード用暗号鍵記憶メモリ19は、書き込み専用であり、外部から読み出しできないハードウェア構成となっていて外部からの不正な暗号鍵の読み出しができないようになっている。このハードウェア構成については前述したのでその説明は省略する。この乗車カード用暗号鍵記憶メモリ19に記憶されている複数の暗号鍵のうち、現在使用されている暗号鍵を用いて乗車カード7処理のための暗号化、復号が行われる。

【0068】また、上位機器である自動改札機1などから現在使用している暗号鍵を変更すべきコマンドが与えられ、その変更コマンドに応じて、図7の現暗号鍵0が、変更すべき暗号鍵に書き換えられ、それまで使用されていた現暗号鍵0が、旧暗号鍵-1となり、それまでの旧暗号鍵-1が、旧暗号鍵-2となり、以下、順送りされた内容に書き換えられ、以後は、この書き換えられた現暗号鍵0を使用して処理が行われる。なお、最も古い暗号鍵は、発行されているすべての乗車カード7で使用される真れがなくなった時点で不要となるので、上書きして消去すればよい。

【0069】また、この実施の形態では、読出／書込機6が使用する暗号鍵は、上位機器からの変更コマンドによって書き換えられるようにしたけれども、本発明の他の実施の形態として、読出／書込機6においても、今後使用する複数の暗号鍵を予め記憶させておき、上位機器からの更新コマンドによって現在使用する暗号鍵を変更するように構成してもよい。

【0070】暗号回路18は、暗号鍵を用いて平文の暗号化、暗号文の復号を行い、また、上位機器とか乗車カード7との通信文（コマンド、レスポンス）の暗号化、復号の他、上位機器と乗車カード7との相互認証においても使用される。乗車カード7は、通常、読出／書込機6との相互認証の終了後にその他のコマンドを受け付けるようになっている。

【0071】次に、自動改札機1における処理を図8で示されるフローチャートを参照して説明する。

【0072】乗車カード7が、改札機本体2の読出／書込機6と通信し得る通信エリア内に無いときは、読出／書込機6は常に10ミリ秒程度の一定周期でポーリングコマンドをアンテナコイル23から送出している（ステップn1）。前記通信エリアに乗車カード7が進入し、その乗車カード7からポーリングコマンドに対するレス

ポンスが返送されると（ステップn2）、読出／書込機6と乗車カード7との間の相互認証を行う（ステップn3）。この相互認証については図9を用いて後で説明する。相互認証がOKであれば、乗車カード7のデータの読み出しと乗車カード7へのデータの書き込みの処理を行い（ステップn4）、最後に読出／書込機6が次の乗車カード7に対するポーリングに対して、処理済みの乗車カード7が応答しないように応答禁止の処理をする（ステップn5）。

【0073】次に図9を参照して前記相互認証について説明する。

【0074】読出／書込機6から乗車カード7に対しランダムデータDrを送出する（ステップn10）。乗車カード7は、該乗車カード7で使用している暗号鍵を用いてそのランダムデータDを暗号化して暗号化データDr'とし、その暗号化したデータDr'を読出／書込機6に送信する。読出／書込機6は、そのデータDr'を受信する一方（ステップn11）、そのランダムデータDrを現在使用している暗号鍵K（0）を用いて暗号化して暗号化データDr'（0）を得る（ステップn12）。そして、読出／書込機6はその暗号化したデータDr'（0）を乗車カード7から送信されてきた暗号化データDr'と比較し（ステップn13）、両データDr'（0）とDr'とが一致していれば乗車カード7が正しい乗車カード7と認証するが、一致しないときは乗車カード7が不正な乗車カード7であるか、それとも乗車カード7が使用している暗号鍵が古い暗号鍵であるかのいずれかとなる。

【0075】乗車カード7が正しい乗車カードと認証した場合、今度は、乗車カード7からランダムデータDcを受信し（ステップn21）、このランダムデータDcを現在使用している暗号鍵K（0）で暗号化し（ステップn22）、暗号化データDc'として、乗車カード7に送出する（ステップn23）。乗車カード7からこの送出に対するレスポンスを受信すると（ステップn24）、受信内容から認証OKの場合は（ステップn25）、相互認証が完了し（ステップn26）、OKでない場合は相互認証NGとする（ステップn27）。

【0076】ステップn13において、乗車カード7が正しい乗車カードと認証しない場合は、読出／書込機6は、暗号鍵の番号を0に初期化（n=0）した上で（ステップn14）、暗号鍵の番号を過去に使用していた古い暗号鍵の番号にし（n=n+1）（ステップn15）、この番号の暗号鍵K（n）を用いてデータを暗号化し（ステップn17）、乗車カード7から返送されてきた暗号文と一致するかを判断する（ステップn18）。一致と判断できるまで、カード読出／書込機6が記憶している古い暗号鍵を順次選択していき（ステップn16）、番号がnの古い暗号鍵でDr'=Dr'（n）となって一致した場合はカード読出／書込機6

は、乗車カード7が使用していた暗号鍵はその番号の旧い暗号鍵K(n)と判断し、乗車カード7に対して、現在使用されている暗号鍵K(0)に更新するように、すなわち、暗号鍵記憶メモリ11のポインタnの暗号鍵を使用している乗車カード7に対して、ポインタ0の暗号鍵に更新するように暗号鍵更新コマンドを送出し（ステップn19）、乗車カード7が使用する暗号鍵をK(0)に更新させてステップn21以降の処理を行って乗車カード7が正当なものであると認証する。

【0077】また、乗車カード7の暗号鍵の更新後、新しい暗号鍵を用いて再度認証を行うようにしても構わない。なお、読出／書込機6が保有する旧い暗号鍵のいずれの暗号鍵でも暗号文が一致しなかったときには、その乗車カード7は不正な乗車カード7と判断する（ステップn20）。

【0078】次に、カード発行機4の読出／書込機6による処理について説明する。

【0079】カード発行機4では、図10で示されているようにポーリング、レスポンス受信、相互認証OKについて図8と同様である。図10で相互認証が終了すると、暗号鍵書き換えコマンドを送信し、乗車カード7の暗号鍵を含むデータの書き換えの処理を行う（ステップn4）。その際、乗車カード7の暗号鍵記憶メモリ11の複数の暗号鍵を、現在使用する暗号鍵と今後使用する予定の複数の暗号鍵に書き換える（ステップn5）。これによって、乗車カード7は、当初は、現在使用する暗号鍵を選択して使用し、以後は、更新コマンドによって使用する暗号鍵を順番に更新する。

【0080】なお、乗車カードが、使用されたカードを回収して発行するのではなく、全く、新規に乗車カードを発行する場合には、相互認証を行うことなく、現在使用する暗号鍵と今後使用する予定の複数の暗号鍵を書き込めばよい。

【0081】上述の実施の形態では、自動改札などの駅務システムに適用したけれども、本発明は、かかるシステムに限定されるものではなく、自動料金徴収システムあるいはその他のシステムにも適用されるものである。

【0082】また、上述の実施の形態では、非接触方式の通信に適用したけれども、本発明は、接触方式の通信にも適用され得る。

【0083】

【発明の効果】以上のように本発明によれば次の効果を得られる。

【0084】請求項1の本発明の記憶媒体によれば、読出／書込機との間の暗号処理において、複数の暗号鍵のいずれかをを用いて暗号処理を行うので、共通暗号鍵方式のように一つの共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を

用いる従来例のように、すべての暗号鍵が傍受されて解読される虞れが低く、セキュリティ性が向上する。

【0085】請求項2の本発明の記憶媒体によれば、複数の暗号鍵の少なくとも一部の暗号鍵を読出／書込機から書き換えることができるので、記憶されている複数の暗号鍵が更新によってすべて使用されてしまうまでに、新たな暗号鍵に書き換えることができ、これによって、永続的に新しい暗号鍵への更新が可能となり、セキュリティ性を永続的に確保できる。

【0086】請求項3の本発明の読出／書込機によれば、記憶媒体が使用している暗号鍵が、過去に使用された暗号鍵であるか否かを判断し、読出／書込機で過去に使用されている暗号鍵であるときには、記憶媒体に更新コマンドを送出して記憶媒体が使用する暗号鍵を更新することができるので、記憶媒体の暗号鍵を、読出／書込機が現在使用している最新の暗号鍵に一致させることができる。したがって、記憶媒体が使用する暗号鍵を変更するために、記憶媒体を回収して暗号鍵を一斉に変更するといった困難な作業を行う必要がなく、記憶媒体が使用されて読出／書込機との間で通信を行うことにより、自動的に暗号鍵が変更されることになる。

【0087】請求項4の本発明の読出／書込機によれば、上位機器からのコマンドによって使用する暗号鍵が変更されるので、必要に応じて、例えば、定期的あるいは現在使用している暗号鍵が解読される虞れがあるような時に、上位機器からのコマンドによって使用する暗号鍵を新しい暗号鍵に変更できることになり、セキュリティ性を確保でき、さらに、請求項3の作用によって、記憶媒体が使用する暗号鍵もその変更された暗号鍵に一致させることができる。

【0088】請求項5の本発明の読出／書込機によれば、記憶媒体が記憶している複数の暗号鍵の少なくとも一部の暗号鍵を書き換えるので、記憶媒体の暗号鍵が順次更新されて記憶されている全ての暗号鍵が使用されてしまうまでに、新たな複数の暗号鍵に書き換えることができ、これによって、永続的に新しい暗号鍵への更新が可能となり、セキュリティ性を永続的に確保できる。

【0089】請求項6の本発明のカードシステムによれば、カードと読出／書込機との暗号鍵が一致しなくても、カードの暗号鍵が、読出／書込機で過去に使用した暗号鍵であれば、カードの暗号鍵が更新されて読出／書込機の暗号鍵に一致するので、相互認証が可能となる。しかも、記憶媒体をカードとしているので、自動料金収集システムなどの各種の用途に好適に実施できることになり、請求項1ないし5の作用効果を顕著に奏することができる。

【0090】請求項7の本発明の暗号鍵使用方法によれば、読出／書込機は、記憶媒体からの暗号化データと作成した暗号化データとを比較することにより、記憶媒体の暗号鍵が、読出／書込機が使用している暗号鍵に一致

しているか否かを判断し、一致していないときには、記憶媒体の暗号鍵が、過去に使用した暗号鍵であるか否かを判断し、過去の暗号鍵であるときには、記憶媒体の暗号鍵を更新させるので、記憶媒体の暗号鍵と読出／書込機との暗号鍵を一致させることができる。

【0091】また、記憶媒体および読出／書込機は、複数の暗号鍵を記憶しているので、一つの共通暗号鍵のみを記憶している共通暗号鍵方式のように共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、すべての暗号鍵が傍受されて解読される虞れが低く、さらに、記憶媒体に記憶されている複数の暗号鍵を一斉に変更するといった必要もない。

【0092】請求項8の本発明の駅務システムによれば、乗車カードと自動改札機の読出／書込機との間の暗号処理において、乗車カードおよび読出／書込機は、複数の暗号鍵を記憶しているので、一つの共通暗号鍵のみを記憶している共通暗号鍵方式のように共通暗号鍵が解読されてもシステム全体のセキュリティ性が損なわれることがなく、また、使用する暗号鍵も読出／書込機からのコマンドによって必要に応じて更新されるので、ランダムにすべての暗号鍵を用いる従来例のように、すべての暗号鍵が傍受されて解読される虞れが低く、さらに、乗車カードに記憶されている複数の暗号鍵を一斉に変更するといった必要もない。

【0093】請求項9の本発明の駅務システムによれば、カード発行機は、乗車カードの発行時に、乗車カードに記憶されている複数の暗号鍵を書き換えるので、永続的に新しい暗号鍵への更新が可能となり、システムのセキュリティ性を永続的に確保できる。

【0094】請求項10の本発明のカード発行機によれば、回収した乗車カードを用いるのではなく、全く新規な乗車カードの発行時において、相互認証などを行うことなく、現在使用する暗号鍵および将来使用する予定の複数の暗号鍵を書き込むとともに、現在使用する暗号鍵を選択するよう設定して乗車カードを発行できる。

【図面の簡単な説明】

【図1】 本発明の実施形態に係るシステムの概略構成図である。

10 【図2】 自動改札機の斜視図である。

【図3】 乗車カードのブロック図である。

【図4】 乗車カードの暗号鍵記憶メモリの記憶内容を示す図である。

【図5】 読出／書込機のブロック図である。

15 【図6】 暗号鍵の使用期間を示す図である。

【図7】 読出／書込機の乗車カード用暗号鍵記憶メモリの記憶内容を示す図である。

【図8】 自動改札機の読出／書込機の動作説明に供するフローチャートである。

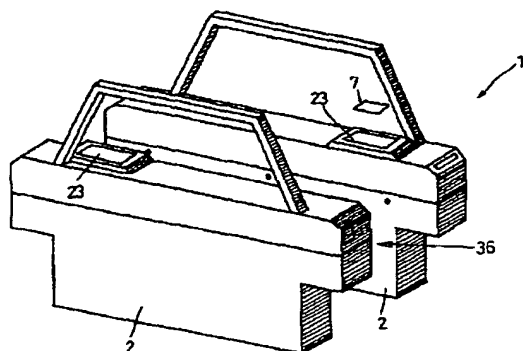
20 【図9】 相互認証の動作説明に供するフローチャートである。

【図10】 カード発行機の読出／書込機の動作説明に供するフローチャートである。

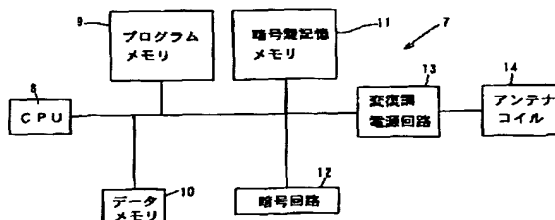
【符号の説明】

- |    |        |                |
|----|--------|----------------|
| 25 | 1      | 自動改札機          |
|    | 6      | 読出／書込機         |
|    | 7      | 乗車カード          |
|    | 8, 15  | CPU            |
|    | 11     | 暗号鍵記憶メモリ       |
| 30 | 14, 23 | アンテナコイル        |
|    | 19     | 乗車カード用暗号鍵記憶メモリ |

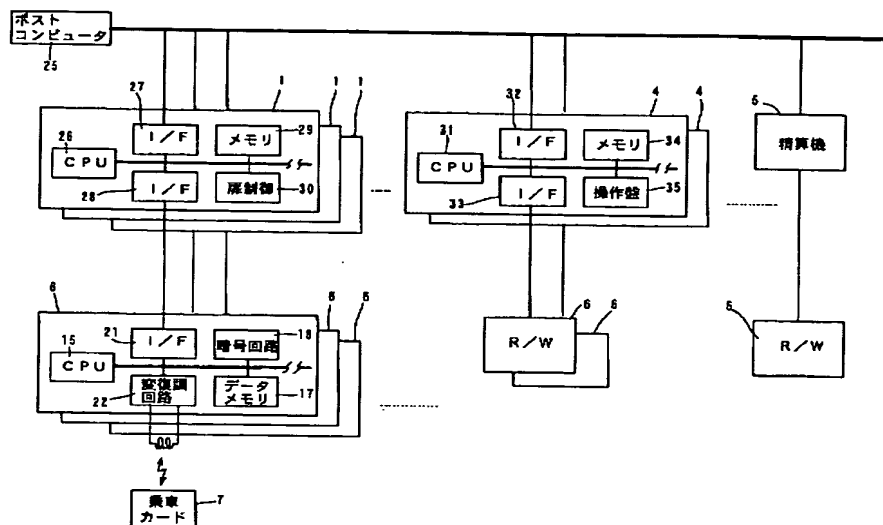
【図2】



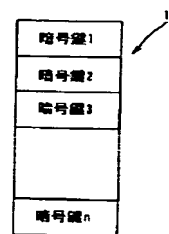
【図3】



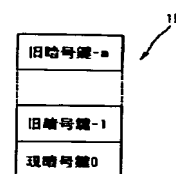
【図1】



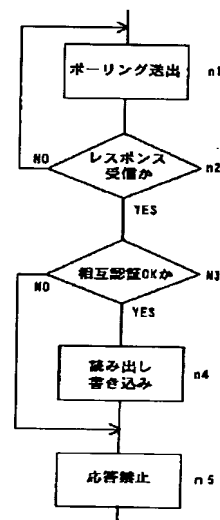
【図4】



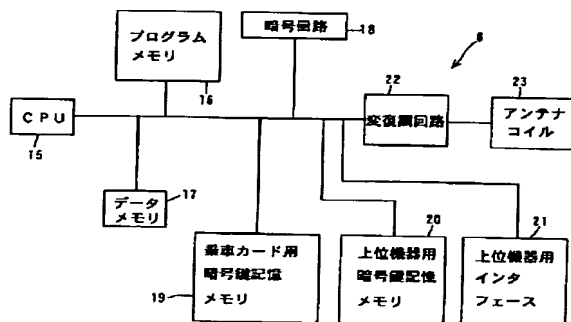
【図7】



【図8】



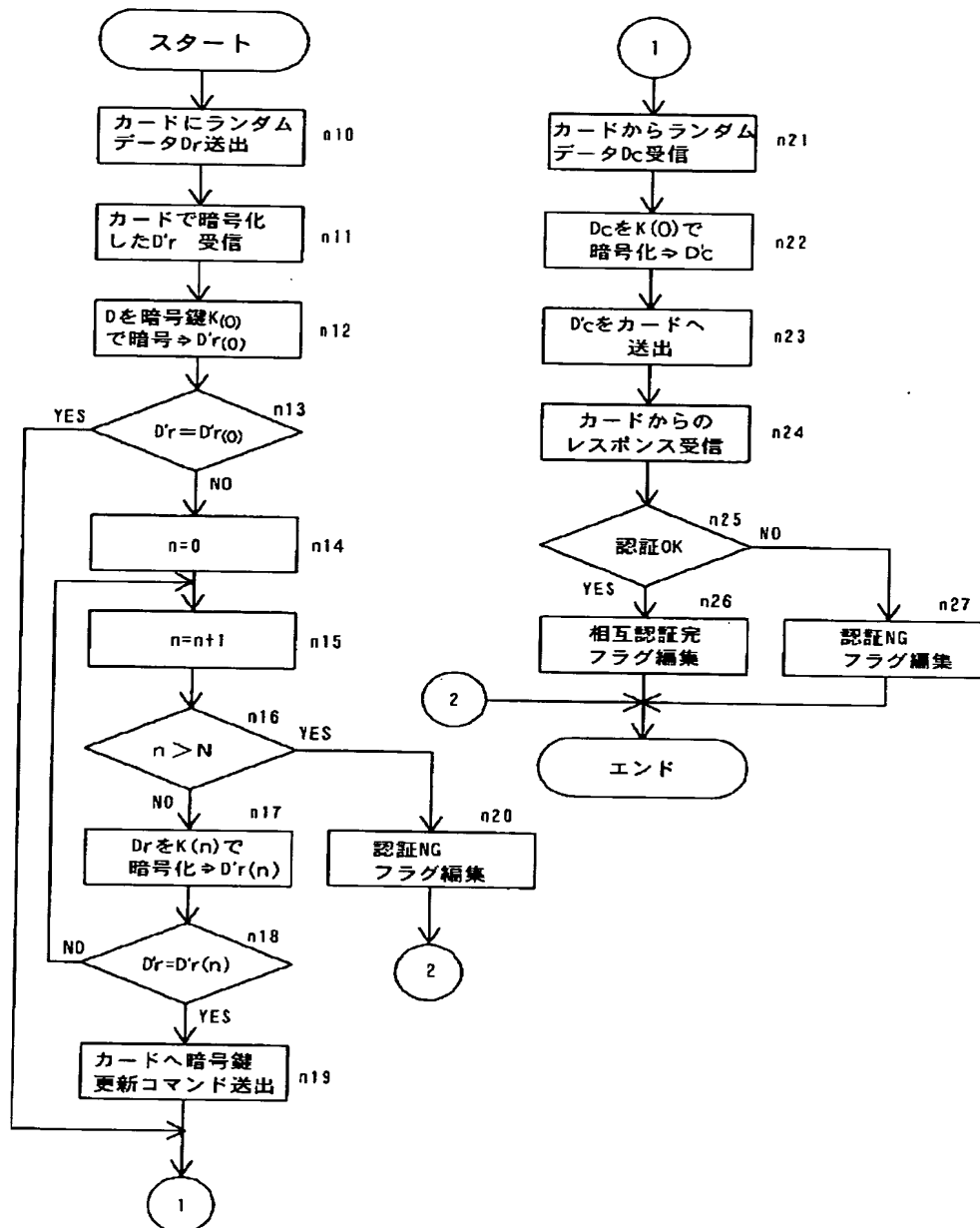
【図5】



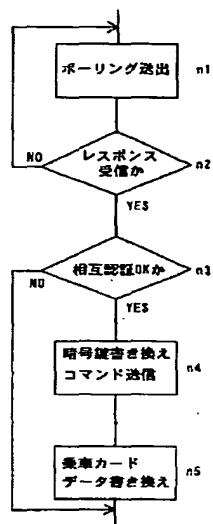
【図6】

暗号鍵	使用期間	状態
暗号鍵1	1998.01.01~ 1998.03.31	過去に使用
暗号鍵2	1998.04.01~ 1998.05.10	現在使用中
...	...	...
暗号鍵n		未使用

【図9】



【図10】



フロントページの続き

(51) Int. Cl.<sup>7</sup>  
H04L 9/32

識別記号

FI  
H04L 9/00

テ-マ-ド\* (参考)

673C